



U.S. Department of Justice

United States Attorney
Southern District of New York

26 Federal Plaza
38th Floor
New York, New York 10278

July 11, 2025

BY EMAIL

The Honorable Katherine Polk Failla
United States District Judge
Southern District of New York
40 Foley Square
New York, New York 10007

Re: *United States v. Roman Storm*, 23 Cr. 430 (KPF)

Dear Judge Failla:

The Government respectfully writes in opposition to the defendant's letter motions, filed this morning, to exclude the contents of Alexey Pertsev's cellphone extraction (the "Pertsev Extraction") from evidence, inspect grand jury minutes, and compel a *Brady* review (the "Motions"). (Dkt. 193). The Motions are meritless distractions that should be denied.

I. THE COURT SHOULD ADMIT THE PERTSEV EXTRACTION RECORDS OBTAINED BY SPECIAL AGENT PETER DICKERMAN

The defendant moves for the exclusion of the records obtained by Special Agent Peter Dickerman in the Netherlands because they include forwarded Telegram messages that do not identify the original author, and they could—in theory—have been modified before Special Agent Dickerman obtained them. As set forth below, this motion is replete with baseless assumptions and wrong on the law. The Court should deny it.

A. Background

Dutch law enforcement made an initial production of four separate chats that had been identified as of particular interest involving Roman Storm from Pertsev's cellphone to the Government on January 13, 2023. This initial production was in the form of HTML files, not the native extractions. On May 25, 2023, Dutch law enforcement provided the extracted versions of those same chats, and all other chats pertaining to Roman Storm from the Pertsev Extraction, in the same form as the files that Special Agent Dickerman later obtained. The Government produced both the initial HTML versions of the four chats initially received from the Dutch, and the extracted versions of all the chats that were subsequently received, in discovery in this case in September 2023.

For the sole purpose of ensuring that the Government would be able to adequately authenticate the chats, on November 6 and 7, 2024, Special Agent Dickerman met with Dutch law enforcement agents in the Netherlands in order to obtain new copies of the same files previously provided by Dutch law enforcement in May 2023—this time, obtained directly from the Pertsev Extraction by an American law enforcement officer. While in the Netherlands, Special Agent Dickerman personally accessed the entirety of the Pertsev Extraction, which was stored on a Dutch law enforcement computer, and obtained from the extraction the full set of chat records previously provided by Dutch law enforcement. The records Special Agent Dickerman obtained are the only records from Pertsev’s cellphone that the Government intends to introduce at trial.¹

B. Nothing Is “Missing” from the Records that Special Agent Dickerman Obtained

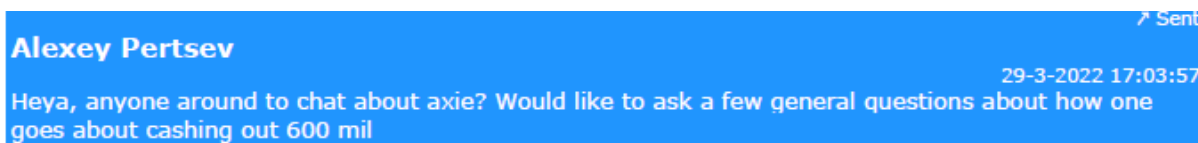
The defendant asserts that the Pertsev Extraction “is missing critical information” because it does not identify the original author of forwarded messages. (Motions at 3). But this assumes that the Pertsev Extraction contains, or should contain, the information that the defendant seeks. This assumption is unfounded. The defendant’s only basis for that claim is a screenshot of a Telegram chat from an unknown source, using an unknown version of Telegram, under unknown user settings. That simply does not establish that Telegram generally reflects the original author of forwarded messages—let alone that it did so on Pertsev’s cellphone in 2022.² Accordingly, the notion that this information is “missing” from the records obtained by Special Agent Dickerman but present on the Pertsev Extraction, or that those records have somehow been altered, has no basis in fact.

Nor are the Telegram chats obtained by Special Agent Dickerman “misleading,” as the defense maintains. (Motions at 4). The defendant focuses on a statement in the Indictment attributing a particular message to CC-1, as well as the Government’s repetition of that at the pretrial conference. But the source of that original attribution is that the Government’s initial receipt of this chat was in the initial HTML version provided by Dutch authorities on January 13,

¹ The defendant claims that Special Agent Dickerman “did *not* return to the United States with all the files he sought to have extracted” from the Pertsev Extraction. (Motion at 1 (emphasis in original)). Like much else in this motion, this claim is irrelevant and false—irrelevant because whether Special Agent Dickerman intended to retrieve a record he left behind has no bearing on whether the evidence “in question is what [the Government] claims,” and false because the very 3500 that the defendant cites explains that the Dutch authorities “did not permit [Special Agent Dickerman] take [a particular file] because they had not previously provided it to the” United States. 3540-016. In other words, Special Agent Dickerman was never authorized to obtain anything more than new copies of what had previously been provided by the Netherlands, and it was never contemplated that Special Agent Dickerman would return with the files that remained in the Netherlands.

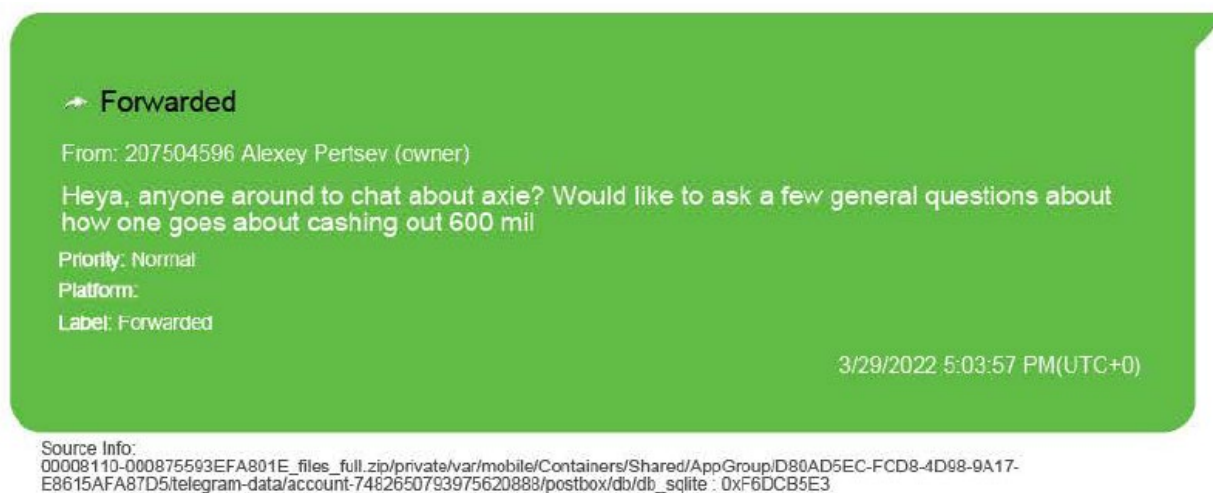
² The Government notes that Telegram contains a feature, and at least one third party provides an add-on to Telegram, that allow anonymous forwarding. See <https://www.junctionbot.io/articles/how-to-hide-the-original-author-of-a-message-when-forwarding-in-telegram>.

2023, as described above, which were formatted in a way that did not indicate that a message had been forwarded, as in the following example:



For the same reason, the original draft translation that was used by the Government did not note that this chat was forwarded, because that was not reflected in the HTML version.

By contrast, the extracted copies of these chats produced by the Dutch in May 2023, as well as the extracted copies of these chats obtained directly by Special Agent Dickerman—the copies that the jury will see—clearly demonstrate when a message has been forwarded, as follows:



Far from calling into question the Dickerman extractions, this illustrates that these extractions contain the full information from the Pertsev phone, unlike the HTML versions that the Government initially received from Dutch authorities, and that there is no risk that these exhibits will confuse the jury about when messages were forwarded.

Moreover, the defendant's motion should be denied as an obvious attempt to ambush the Court and the Government three days before trial. As described above, the Government initially obtained the extracted versions of the chats from the Dutch, which are the same as the versions extracted by Dickerman, and produced those in discovery in September 2023. Thus, the defense has had nearly two years to review this discovery and identify messages that have been forwarded, especially messages that were particularly noticed to the defense by being included in the Indictment. The defense has also had the Dickerman version of these extractions since December 2024. The suggestion that this issue could not have been previously discovered is simply incorrect.

Lastly, the defendant is mistaken that messages forwarded by the defendant and his co-conspirators are categorically "not [] co-conspirator statements." (Motions at 3) Opposing-party statements—including those of co-conspirators—are not hearsay when they are statements that the

declarant “manifested [and] adopted or believed to be true.” Fed. R. Evid. 803(d)(2)(B), (E). The message in which Pertsev forwarded a reporter’s statement that he “[w]ould like to ask a few general questions about how one goes about cashing out 600 mil” is precisely such a message. GX 2044-T at 9. Pertsev forwarded the message to his co-conspirators shortly after news of the Ronin hack broke, in a discussion begun by Roman Semenov’s message, “Did you already see the \$600,000,000 hack today? Shit might seriously hit the fan now.” *Id.* at 4. That is, Semenov had already highlighted the likelihood that the Ronin hack would connect to Tornado Cash, and Pertsev then forwarded a message consistent with that expectation. Nobody in this discussion, including Pertsev, expressed any skepticism that the hackers would use Tornado Cash. Indeed, Pertsev did not deny the obvious import of the reporter’s message: that the way one goes about cashing out \$600 million is through Tornado Cash. He did not deny it because it was true, and everyone in the chat knew it was true. Instead, Pertsev merely announced, “We’re being contacted by CoinDesk.” *Id.* at 9. Pertsev’s conveyance of the message adopted the import of it; that when a large hack like this happened, discussion of “cashing it out” would involve Tornado Cash. The message is also independently admissible because it put the defendant on notice of a fact that bears directly on intent and willfulness with respect to the charged offenses—namely, that it was widely and openly known in the cryptocurrency world that when large hacks happened, Tornado Cash would be used to launder the proceeds.

C. The Fact that the Files Special Agent Dickerman Obtained Theoretically Could Have Been Modified Is No Basis for Exclusion and Stands in Stark Contrast to the Abundant Indicia of Authenticity the Government Will Offer at Trial.

The defendant leaps from the “possibility” that the GrayKey report “could have” been modified to the conclusion that “what the report claims is Pertsev’s phone is not.” (Motions at 1). Similarly, he argues that, if the other files that Special Agent Dickerman brought back from the Netherlands are “able to be modified, then Agent Dickerman cannot say that [they are] what the government claims [them] to be.” (Motions at 6). Both arguments are meritless for the same fundamental reason: there is no basis—and the defendant provides none—to even speculate that the records were altered. To the contrary, there are multiple bases to authenticate the files obtained by Special Agent Dickerman (i.e., from the Pertsev Extraction), far exceeding the standard that courts have recognized is necessary for authentication purposes.

With respect to the GrayKey report, the defendant laments that the report theoretically could have been altered and that there is a forensic tool for detecting alterations in PDFs that the Government may not have employed. (Motions at 6). What the defendant conceals—although he knows it because the Government produced this information—is that the Government analyzed the authenticity of the GrayKey report by examining its metadata, which indicates that no modifications have been made. *See* 3540-017. Specifically, the “Modified” metadata field is blank, and the “Created” field reflects that the document was created on August 11, 2022 at 12:25:10 AM,³ eleven seconds after an entry on the face of the GrayKey report indicates that the report was

³ The metadata contains two sets of “Created” and “Modified” fields—one in the “Document Properties” window and another in the “Additional Metadata” window. Both sets on the GrayKey report indicate that there have been no modifications. The “Document Properties” window

generated—a time difference that the Government understands is negligible.⁴ Accordingly, even though there is no reason to believe the GrayKey report was modified, the Government has analyzed the GrayKey report for modifications and found none.

Regarding the Pertsev Extraction, the Government intends to present at trial no fewer than five means of authentication, each of which would be sufficient on its own to support authentication. Taken together, these methods of authentication are amply sufficient.

A. Applicable Law

“[T]he requirement of authenticati[on] . . . [is satisfied by] evidence sufficient to support a finding that the matter in question is what its proponent claims.” Fed. R. Evid. 901(a). The bar for authentication “is not particularly high.” *United States v. Bout*, 651 F. App’x 62, 63 (2d Cir. 2016). Indeed, evidence is properly authenticated as long as a reasonable juror could find in favor of authenticity. *See United States v. Tin Yat Chin*, 371 F.3d 31, 38 (2d Cir. 2004). The proponent need not “rule out all possibilities inconsistent with authenticity, or to prove beyond any doubt that the evidence is what it purports to be. Rather, the standard for authentication, and hence for admissibility, is one of reasonable likelihood.” *United States v. Pluta*, 176 F.3d 43, 49 (2d Cir. 1999).

As described in Rule 901, a proponent may authenticate evidence in multiple ways, including, for example, “[t]estimony that an item is what it is claimed to be”; “[t]he appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances”; and “[e]vidence describing a process or system and showing that it produces an accurate result.” Fed. R. Evid. 901(b)(1), (4), (9). In other words, evidence of authenticity “may be direct or circumstantial, and the latter category may include distinctive characteristics of the document itself.” *United States v. Maldonado-Rivera*, 922 F.2d 934, 957 (2d Cir. 1990). “With respect to a document attributed to the defendant, the prosecution need only provide a rational basis from which the jury could infer the document did, in fact, belong to him.” *Id.*

B. Five Methods of Authentication

First, the GrayKey report, GX 2300, contains machine-generated identifying information from the cellphone that was extracted. This information authenticates that this cellphone was

indicates that the report was created on August 10, 2022 at 6:25:10 PM. The Government understands that the “Document Properties” window expresses time in the local time zone of the computer on which the file currently is open, whereas the “Additional Metadata” window expresses time in Universal Time Coordinated. This comports with the six-hour time difference between the two metadata entries.

⁴ The face of the GrayKey report contains two entries that read “progress report generated,” approximately four minutes apart. Special Agent Dickerman is expected to testify that he has seen this numerous times in his experience and that he has not seen it result in any errors in the data that the GrayKey report contains regarding the authenticity of the extraction.

Alexey Pertsev’s cellphone in the following ways: (1) it reflects the account name, device serial number, IMEI numbers, owner/user name, and phone number ending in -9003 listed in the subscriber information for the Pertsev.One@gmail.com iCloud account, *see* GX 403 (Registrations Account Tab, Row 16); (2) it reflects the account name and phone number ending in -2208 that is listed in the subscriber information of an iCloud account that belongs to Pertsev, for which his user name is Peppersec@yandex.ru, *see* GX 413; and (3) its hash values correspond to those of the Pertsev Extraction.⁵

Second, the Government will present a comparison between the following six files from the Pertsev Extraction and substantively identical copies of the same files from an iCloud account that belongs to Pertsev:

File Description	From Pertsev Extraction	From Pertsev.One@gmail.com iCloud
Video of Pertsev in Tornado Cash Clothing 1	GX 2400	GX 441
Video of Pertsev in Tornado Cash Clothing 2	GX 2401	GX 442
Photo of Pertsev’s Russian Passport	GX 2403	GX 417
Photo of Pertsev and Female	GX 2402	GX 429
Photo of Pertsev in Tornado Cash Clothing	GX 2404	GX 438
Photo Tornado Cash Clothing	GX 2405	GX 437

Third, Special Agent Dickerman is expected to testify that the Pertsev Extraction contains a copy of a Telegram chat among the defendant, his co-conspirators, and their investors at Dragonfly Capital that matches a copy of the same chat the Government obtained directly from Dragonfly Capital. *See* GX 2240-79 (from the Pertsev Extraction), GX 1363-75 (from Dragonfly Capital).

Fourth, the Government expects that Special Agent Dickerman will testify that the Pertsev Extraction contains a copy of a Telegram chat among a partner at the law firm, McDermott Will & Emery (“McDermott”), the defendant, and his co-founders, a copy of which the Government also obtained directly from McDermott. *See* GX 2070 (from the Pertsev Extraction), GX 1006 (from McDermott). In that chat, the McDermott attorney contacted the defendant and his co-founders to seek help on behalf of a client that had been victimized by the Tornado Cash service. He received a false, stock response that there was no way for the Tornado Cash service to help.

⁵ The Government notes that, if the Pertsev Extraction had been modified, its hash values would have automatically changed. To the extent the defendant wishes to allege—without any basis—that someone altered the Pertsev Extraction, he would have to also allege that they altered the hash value of the GrayKey report whose metadata shows no alterations.

The McDermott attorney is also expected to testify at trial that these messages are indeed messages he sent to the Tornado Cash founders.

Fifth, Special Agent Dickerman is expected to testify that he saw numerous files on the full Pertsev Extraction when he examined it in the Netherlands that further attribute the extraction to Pertsev, including photographs of Pertsev’s Netherlands driver’s license, Pertsev’s Russian passport, Pertsev’s domestic Russian identification, and Pertsev’s Greek visa—as well as numerous photos of Pertsev himself.

C. Discussion

The five means of authentication above far exceed what courts have recognized is sufficient to authenticate records of a device extraction without testimony from the analyst who performed the extraction. *See, e.g., United States v. Jean-Claude*, No. 18-CR-601 (PGG), 2022 WL 2334509, at *23 (S.D.N.Y. June 27, 2022) (tying a cellphone extraction to a forensic image based on a match between the IMEI number reflected in the forensic image and the IMEI number reflected on the cellphone’s SIM card tray, where, unlike here, the testifying witness did not obtain the records at issue directly from the extraction); *United States v. Balouchzehi*, No. 23-7609-CR, 2024 WL 4586526, at *2 (2d Cir. Oct. 28, 2024) (affirming authentication based on testimony that the data did not appear to be modified, that the make and model of the device matched those listed in the extraction, and that the extraction contained photos of the defendant—far less than the Government offers here). There is no reason for the Court to impose a higher standard in this case.

The Government acknowledges that the Pertsev Extraction and GrayKey report each hypothetically *could have* been modified, *theoretically*. But that is exceedingly unlikely given the metadata of the GrayKey report and the matching hash values—which are routinely used by forensic examiners for just this purpose, to confirm that files were not modified from their original form—of the Pertsev Extraction and GrayKey report. The exceedingly small, hypothetical possibility that the files were somehow modified in corresponding ways to prevent detection is nowhere near sufficient to prevent authentication, for which the party offering evidence need not “rule out all possibilities inconsistent with authenticity, or to prove beyond any doubt that the evidence is what it purports to be.” *Pluta*, 176 F.3d at 49; *see also Jean-Claude*, 2022 WL 2334509, at *22 (authenticating cellphone records over the defense’s objection that a SIM card tray reflecting the cellphone’s IMEI number could have been removed and replaced). Nor should any chain of custody objection bear on the authentication of the Pertsev Extraction records, as chain of custody goes to weight—not admissibility. *See United States v. Bout*, 651 F. App’x 62, 64 (2d Cir. 2016) (“Alleged breaks in the chain typically do not bear upon the admissibility of evidence, only the weight of the evidence.” (internal quotation marks omitted)).

In sum, the defendant has provided no valid basis to question the authenticity of the records Special Agent Dickerman obtained in the Netherlands. Accordingly, the defendant’s motion for exclusion should be denied.

II. THE COURT SHOULD DENY THE DEFENDANT’S MOTION TO INSPECT THE GRAND JURY MINUTES IN THIS CASE

The defendant moves for disclosure of the grand jury minutes underlying the Indictment and Superseding Indictment based on the Indictment’s supposed misrepresentation of the author of the Telegram message discussed above, sent to the defendant by the defendant’s co-conspirator, Alexey Pertsev, regarding the Ronin Hack. In particular, the defendant takes issue with the following language from the Indictment: “Later that day, CC-1 sent a message to STORM and SEMENOV through the Encrypted App, saying ‘Heya, anyone around to chat about axie? Would like to ask a few general questions about how one goes about cashing out 600 mil.’” Ind. ¶ 57. CC-1 is Pertsev. The defense is correct that this message was in fact a message that Pertsev forwarded from a journalist to the defendant and Semenov in their long-running Telegram chat—this is readily apparent from the Dickerman extraction, which illustrates why the defense’s attempts to suggest that the extraction is somehow “misleading” are meritless. The defendant claims that the Government falsely attributed this statement to Pertsev in the Indictment, calling into question the veracity of the evidence presented to the grand jury. This argument is meritless and thus the Court should not order the Government to disclose any grand jury minutes and compromise the grand jury’s secrecy.

1. Applicable Law

“The burden on a party seeking disclosure of grand jury materials is high,” *United States v. Kirton*, No. 20 Cr. 322 (PMH), 2021 WL 1550423, at *1 (S.D.N.Y. Apr. 20, 2021), and disclosure of grand jury materials “is an extraordinary remedy,” *United States v. Lesane*, No. 22 Cr. 110 (VSB), 2023 WL 155538, at *9 (S.D.N.Y. Jan. 13, 2023), *reconsideration denied*, No. 22 Cr. 110 (LJL), 2023 WL 3560549 (S.D.N.Y. May 19, 2023). “An indictment returned by a legally constituted and unbiased grand jury, . . . if valid on its face, is enough to call for trial of the charges on the merits.” *Costello v. United States*, 350 U.S. 359, 363 (1956); *see also United States v. Williams*, 504 U.S. 36, 54 (1992). As a general matter, there is a presumption of regularity that attaches to grand jury proceedings. *United States v. Mechanik*, 475 U.S. 66, 75 (1986); *Hamling v. United States*, 418 U.S. 87, 139 n.23 (1974) ; *United States v. Leung*, 40 F.3d 577, 581 (2d Cir. 1994); *Torres*, 901 F.2d at 232-33. Thus, “[a] review of grand jury minutes is rarely permitted without specific factual allegations of government misconduct.” *Torres*, 901 F.2d at 233; *see also Leung*, 40 F.3d at 582 (“A review of grand jury minutes should not be permitted without concrete allegations of Government misconduct.”).

At the same time, “[t]here is a tradition in the United States, a tradition that is ‘older than our Nation itself,’ that proceedings before a grand jury shall generally remain secret.” *In re Petition of Craig*, 131 F.3d 99, 101 (2d Cir. 1997) (quoting *Pittsburgh Plate Glass Co. v. United States*, 360 U.S. 395, 399 (1959)). As the Supreme Court has explained, grand jury secrecy is central to our criminal justice system, because “[t]he grand jury as a public institution serving the community might suffer if those testifying today knew that the secrecy of their testimony would be lifted tomorrow.” *United States v. Procter & Gamble Co.*, 356 U.S. 677, 682 (1958). Because of the “indispensable secrecy of grand jury proceedings,” *United States v. Johnson*, 319 U.S. 503, 513 (1943), disclosure is permissible only “where there is a compelling necessity.” *Procter & Gamble Co.*, 356 U.S. at 681.

This principle of grand jury secrecy is codified in Federal Rule of Criminal Procedure 6(e), which, with certain exceptions, instructs most participants in the grand jury process that they “must not disclose a matter occurring before the grand jury.” Fed. R. Crim. P. 6(e)(2)(B). The Rule provides, however, that “[t]he court may authorize disclosure—at a time, in a manner, and subject to any other conditions that it directs—of a grand-jury matter . . . at the request of a defendant who shows that a ground may exist to dismiss the indictment because of a matter that occurred before the grand jury.” Fed. R. Crim. P. 6(e)(3)(E)(ii). “[T]he burden is on the party seeking disclosure to show a ‘particularized need’ that outweighs the need for secrecy.” *United States v. Moten*, 582 F.2d 654, 662 (2d Cir. 1978).

The Supreme Court has “consistently construed [Rule 6(e)] . . . to require a strong showing of particularized need for grand jury materials before any disclosure will be permitted.” *United States v. Sells Engineering*, 463 U.S. 418, 443 (1983); *accord Moten*, 582 F.2d at 662 (a defendant seeking disclosure of grand jury minutes because of a matter that occurred before the grand jury must “show a particularized need that outweighs the government’s strong interest in secrecy”). In order to obtain disclosure, “a defendant must demonstrate some grossly prejudicial irregularity or some other particularized need or compelling necessity that outweighs the Government’s and the Grand Jury’s substantial interest in secrecy.” *United States v. Helbrans*, 547 F. Supp. 3d 409, 434 (S.D.N.Y. 2021) (citing *Gibson*, 175 F. Supp. 2d at 534 and *Sells Eng’g, Inc.*, 463 U.S. at 443). The same showing is required where the defendant seeks *in camera* review of grand jury minutes. *See Torres*, 901 F.2d at 233 (noting that *in camera* “review of grand jury minutes is rarely permitted without specific factual allegations of government misconduct” (citation omitted)); *United States v. Ruiz*, 702 F. Supp. 1066, 1073 (S.D.N.Y. 1989) (requiring a showing of particularized need where defendant requests *in camera* review of grand jury minutes), *aff’d*, 894 F.2d 501 (2d Cir. 1990); *Carter*, 2005 WL 180914, at *5 (“This standard applies to *in camera* review of grand jury proceedings as well as disclosure to parties.”). A district court adjudicating a motion for the disclosure of grand jury materials is “infused with substantial discretion.” *Douglas Oil*, 441 U.S. at 223.

2. Discussion

First, as a factual matter, the allegation in the Indictment that the defendant now challenges is not factually inaccurate. The message that Pertsev sent the defendant and Semenov does in fact “say” what it says. Perhaps the Indictment could have been clearer about the origin of the language Pertsev forwarded to the defendant, but that does not mean it was misleading or false to characterize the message as saying what it says—especially given that, as explained below, the statement was plainly adopted by Pertsev. And by no means does this lack of clarity rise to the level of a “compelling necessity” to look behind the veil of grand jury secrecy. *Procter & Gamble Co.*, 356 U.S. at 681.

Second, regardless of who actually typed out that message, its relevance remains the same: it demonstrates the defendant’s knowledge of the Ronin Hack and the likelihood that Tornado Cash would be used in connection with it. Furthermore, as set forth above, Pertsev’s message—again, regardless of who actually wrote it—is admissible as a co-conspirator statement under Rule 801(d)(2)(E), an adopted admission by the defendant under Rule 801(d)(2)(B), and because it is

not hearsay at all, as it goes to the defendant's knowledge and not the truth of the matter asserted.⁶

Third, as set forth above, the fact that Pertsev forwarded a question from a journalist rather than posing the question himself was something that the defense could have discovered and moved on nearly two years ago, when the Dutch-produced extracted contents of Pertsev's phone were produced, or more than six months ago, when the Special Agent Dickerman-extracted contents of Pertsev's phone were produced. The defendant's seizing on this issue now, just three days before trial, is plainly strategic and comes only after the Court has issued a preliminary ruling indicating that Special Agent Dickerson's testimony will be sufficient to authenticate the contents of Pertsev's phone, including this message exchange. The Court should not reward the defendant's failure to review his own discovery and/or strategic decision to play "gotcha" on the eve of trial in an effort to keep out plainly incriminating evidence.

United States v. Shvartsman, 722 F. Supp. 3d 276 (S.D.N.Y. 2024), a case before United States District Judge Lewis J. Liman, is instructive here. There, Shvartsman moved to dismiss an indictment charging him with various securities fraud charges based on, among other things, the indictment's "quot[ation of] an apparently incriminating text that [a co-defendant] sent him" that the Government later admitted did not pertain to the scheme at issue. *Id.* at 302. In response to a defense motion, the Government provided Judge Liman with the minutes of the grand jury that issued the indictment for his *in camera* review. *Id.* In rejecting Shvartsman's motion to dismiss based on the erroneous inclusion of the text message in the original indictment, Judge Liman found, after reviewing the grand jury minutes for the original indictment, "that the alleged inaccuracies did not substantially influence the grand jury's decision to indict....[and] that the misleading text message was not material to the grand jury's decision to indict, so the Government's presentation of that message to the original grand jury was not prejudicial." *Id.* at 303 (internal editing, quotation, and citations omitted). Here, the Court need not even review the grand jury minutes *in camera* to make this determination. The relevant chat is evidence of the defendant's knowledge of the Ronin Hack and that he and his co-conspirators knew the Lazarus Group was likely to launder the proceeds through the defendant's business, the Tornado Cash service; who authored it is beside the point. Accordingly, the defendant has failed to make a "strong showing of particularized need for grand jury materials," even in the context of an *in camera* review. *Sells Engineering*, 463 U.S. at 443; *see also Torres*, 901 F.2d at 233; *Ruiz*, 702 F. Supp. at 1073; *Carter*, 2005 WL 180914, at *5. For all of these reasons, the Court should deny the defendant's motion to inspect any grand jury minutes in this matter. The Government is, however, prepared to provide the grand jury minutes to the Court for *in camera* review should the Court determine that such review is necessary.

⁶ Even if the Indictment is incorrect (which, on its face, it is not), the Government's error was inadvertent. The original HTML version of this chat that the Government received from Dutch law enforcement and had translated—pictured *supra* Section I.B, did not indicate that Pertsev had forwarded the question from the journalist. The Government did not receive a version of the chat where it was clear that Pertsev was forwarding someone else's message until approximately May 25, 2023, which it promptly produced to the defense on September 26, 2023.

III. THE GOVERNMENT CANNOT BE ORDERED TO CONDUCT A BRADY REVIEW OF THE ENTIRE PERTSEV EXTRACTION BECAUSE THAT EXTRACTION IS NOT WITHIN THE GOVERNMENT’S POSSESSION, CUSTODY, OR CONTROL


The defendant seeks to exclude all evidence from the Pertsev phone based on the Government’s supposed “failure to obtain access to the full extraction” held by Dutch law enforcement, which, according to the defendant, “means that the government cannot conduct a thorough *Brady* review.” (Motions at 6). The trouble with this argument is that it is well-established that “the Government’s *Brady* obligation covers information only in its possession or control” and “does not impose an affirmative duty upon the government to take action to discover information which it does not possess.” *United States v. Colello*, 2024 WL 3429464, at *2 (S.D.N.Y. July 15, 2024). As the Government has explained to counsel and the Court, the full extraction of the Pertsev phone was never in Government’s possession, custody, or control. Rather, it has always been in the possession, custody, and control of Dutch law enforcement, which the Government has no ability to force to do anything. The Government has produced the entirety of the materials that are in its possession. That ends the inquiry and provides no basis to exclude evidence from the Pertsev phone. *See, e.g., United States v. Connolly*, No. 16 Cr. 370 (CM), 2017 WL 945934, at *10 (S.D.N.Y. Mar. 2, 2017) (“[I]f the [British Serious Fraud Office] responded to the MLAT by providing the Government with material from its files, then those documents must be combed for *Brady* materials simply because the Government has the documents in its possession. But I, like the Third Circuit in *Reyerros*, reject the notion that investigatory cooperation—even close cooperation—between the United States and a foreign sovereign could require the Department of Justice to produce documents from a foreign entity—at the risk of dismissal of the Indictment—if the foreign sovereign (unlike a state or federal agency) declines to be treated like an arm of the Government for *Brady* purposes.”) (citing *United States v. Reyeros*, 537 F.3d 270 (3d Cir. 2008); *see also United States v. Ellison*, 527 F. Supp. 3d 161, 166 (D.P.R. 2021) (“The scope of the government’s ‘possession, custody, or control’ is bounded. It does not generally include, for example, information held by...foreign governments.”) (citing *United States v. Hughes*, 211 F.3d 676, 688–89 (1st Cir. 2000); *United States v. Hall*, 171 F.3d 1133, 1145 (8th Cir. 1999); *United States v. Hamilton*, 107 F.3d 499, 509 n.5 (7th Cir. 1997)); *United States v. Lobo-Lopez*, No. 1:08CR194, 2009 WL 10727106, at *1 (E.D. Va. Feb. 26, 2009) (“[D]efendants seek to require the government to conduct a sweeping investigation to determine whether any government agent, agency (whether state, local, or foreign), or government witnesses knows of any exculpatory evidence. *Brady* and its progeny impose no such sweeping production or investigatory obligation.”) (citing *Kyles v. Whitley*, 514 U.S. 419, 437 (1995); *United States v. Graham*, 484 F.3d 413, 417 (6th Cir. 2007) *United States v. Kern*, 12 F.3d 122, 126 (8th Cir. 1993)). Moreover, Storm’s suggestion that there may be *Brady* materials on other portions of the Pertsev phone that are *not* in the Government’s possession is pure speculation—the Government is aware of none and Storm makes no particularized showing suggesting there would be any.

CONCLUSION

For the foregoing reasons, the Motions should be denied.

Respectfully submitted,

JAY CLAYTON
United States Attorney

By: 

Ben Arad
Thane Rehn
Benjamin A. Gianforti
Assistant United States Attorneys
(212) 637-6521
(212) 637-2490
(212) 637-2354

Kevin Mosley
Special Assistant United States Attorney